



QUALYS SECURITY CONFERENCE 2018

Qualys Container Security

Comprehensive Security for the ever-changing Container Stack

Agenda

Container Advantages

Container Deployments

Visibility & Control Challenges

Qualys Container Security Solution

Demo

Q&A

Everybody Loves Containers



Portability

Agility

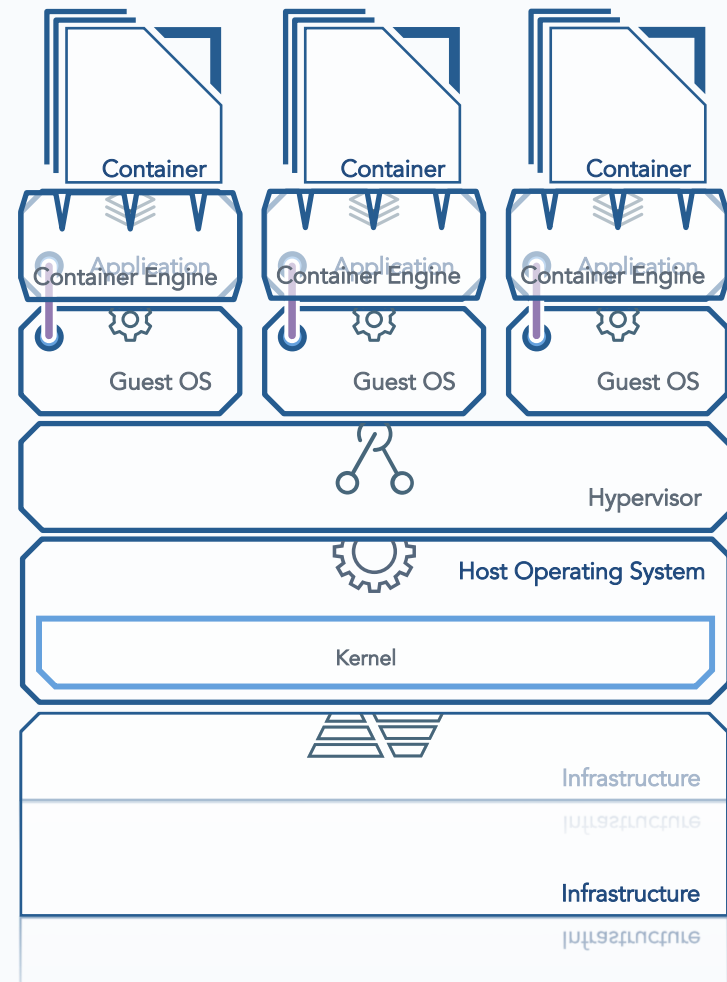
Density

Container Deployments

Deployment Scenario #1

Use Case

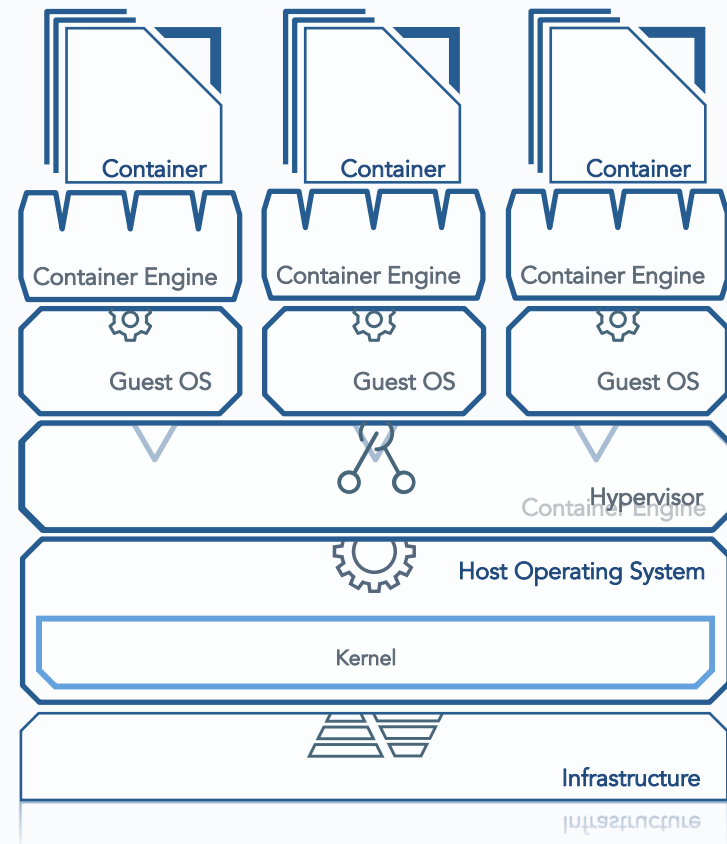
1. Shrinking infrastructure, as organizations continue migration to the cloud
2. Containers deployed within Virtual Machines
3. But organizations still have the overhead and costs of the hypervisor and virtual machines



Deployment Scenario #2

Use Case

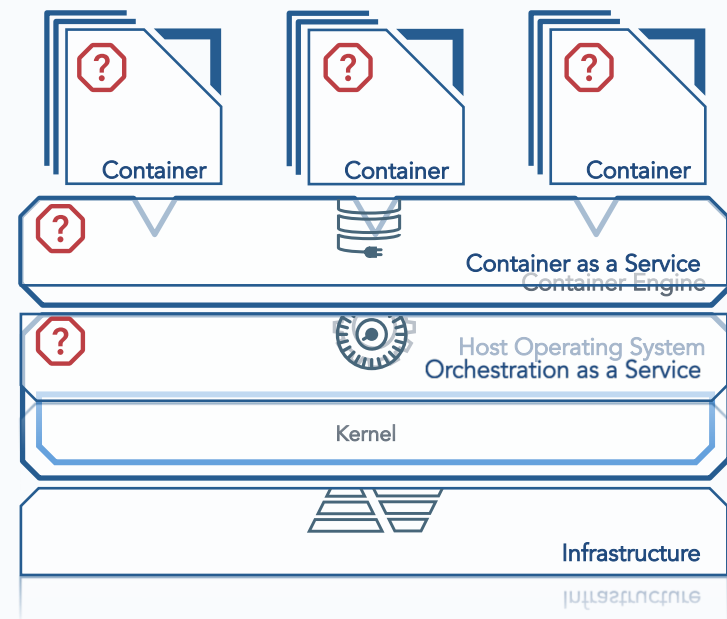
1. The orchestration battle ends with Kubernetes winning 80% of the market
2. But organizations struggle to scale their own Kubernetes clusters



Deployment Scenario #3

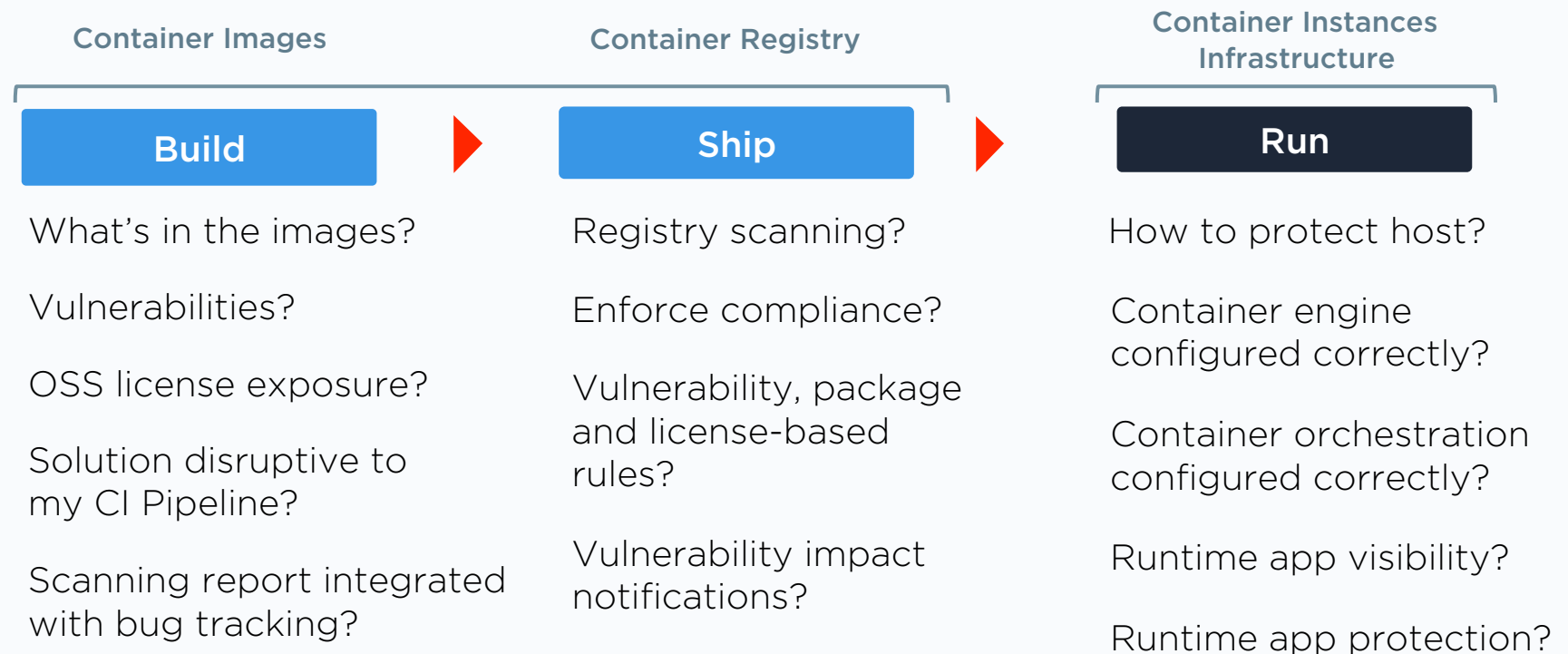
Use Case

1. Container-as-a-Service and Orchestration-as-a-Service adoption accelerate container adoption
2. Now where do you put security?



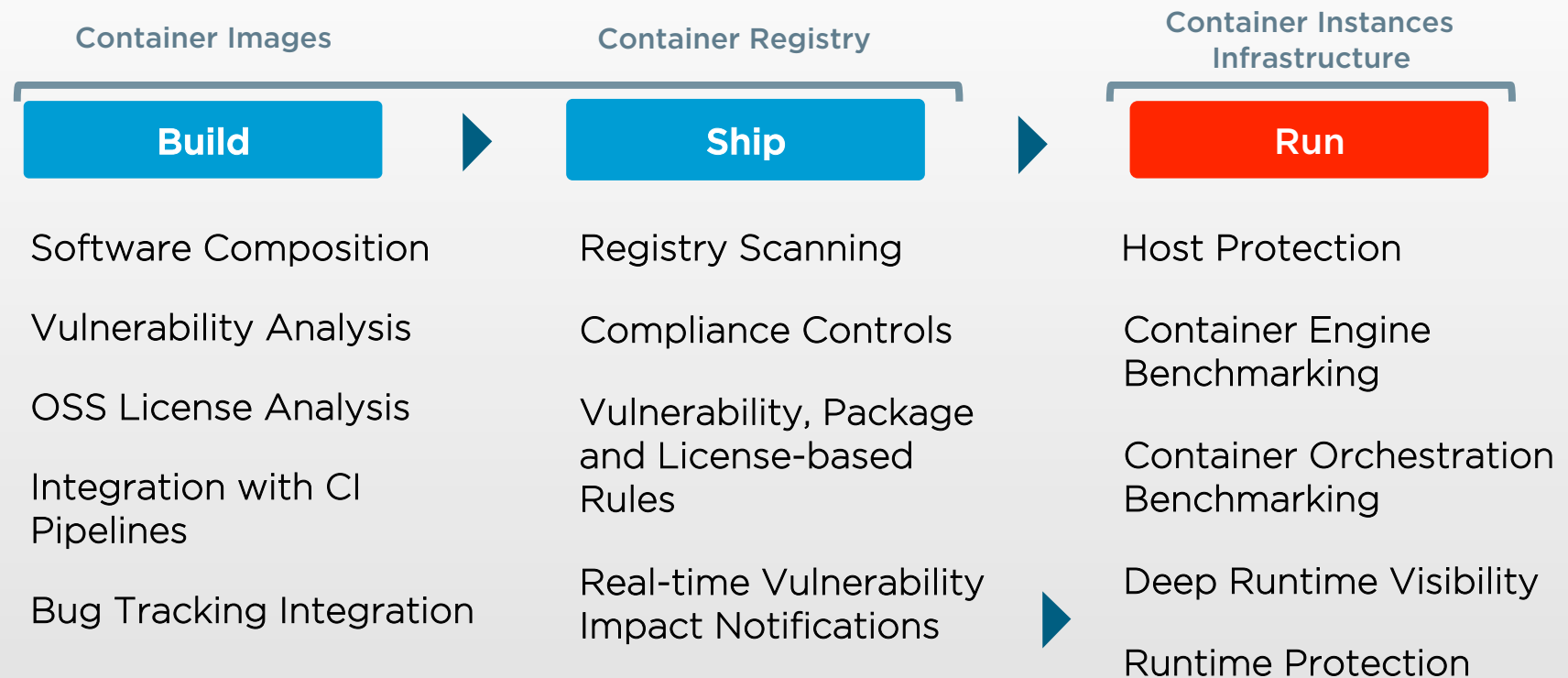
Container Visibility & Security Challenges

Container Lifecycle Challenges



Qualys Container Security

Qualys Container Security



Qualys Container Security

Host Protection

CIS Benchmarks

Protection for container
infrastructure stack

Scanning & Compliance

Accurate insight and control
of container images

Visibility & Protection

Automated analysis and
enforcement of container behavior

Demo

- Dashboard >
- Images >
- Vulnerabilities >
- Containers >
- Policies >
- Settings

Metrics Activity Monitor Topology

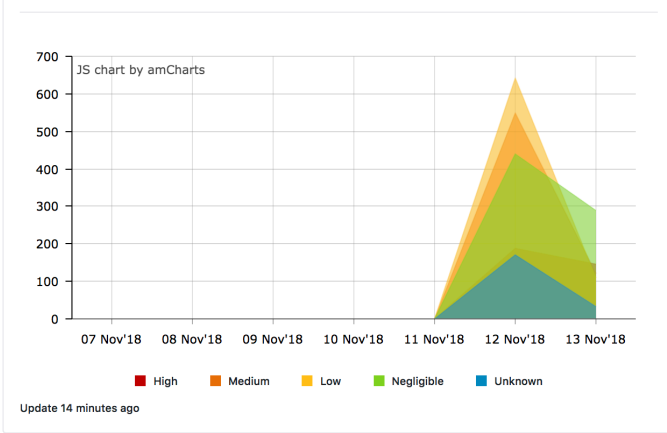
Date Range  Last 7 Days

Assessment Metrics

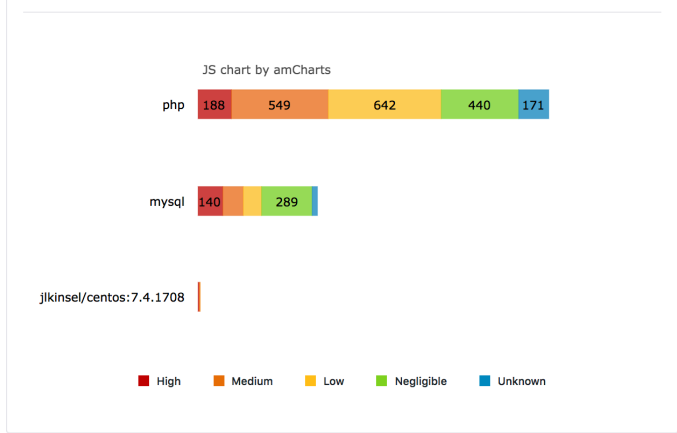
All Vulnerabilities (Last 7 Days)



Vulnerabilities by Severity



Top 5 Most Vulnerable Container Images



Warning 23
High 3

All Images (3)

Add Registry

Name *

Registry name

Location *

Location

Type *

--Select Registry Type--

- Private
- ✓ Docker Hub
- ECR
- DTR

Username *

AWS_ACCESS_KEY_ID

Password *

AWS_SECRET_ACCESS_KEY

Save

Cancel

Search

Quick Links



JK

Search

Add Registry

Add Image

Action



All Images (3)

Add Image

Name *

Registry *

John's DH (docker.io)

Description

Save

Cancel

Search

Quick Links



JK

Search

Add Registry

Add Image

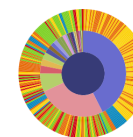
Action



All Images (3)

php

Scan Status: done
Instrumentation Status: Not Instrumented

[Actions ▾](#)

jlkinsel/centos:7.4.1708

Scan Status: done
Instrumentation Status: Active

[Actions ▾](#)

mysql

Scan Status: done
Instrumentation Status: Not Instrumented

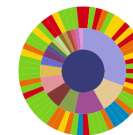
[Actions ▾](#)

Image Details: php

Detail

Scan Date 2018-11-12T23:47:19.2Z

Scan Status done

Registry 5be9e64b9d20760001014780

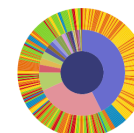
Image Tags

Compliance

Layers

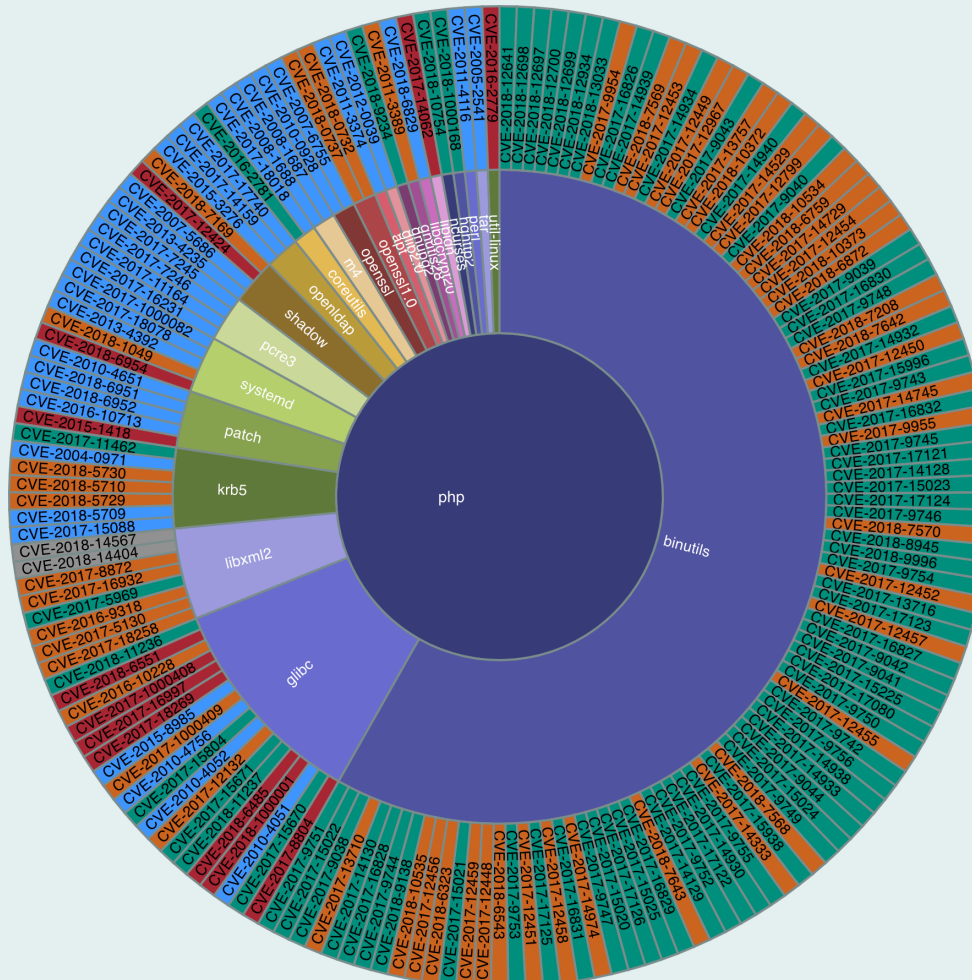
Compliance Sunburst

Vulnerability Sunburst



Total Vulnerabilities: 273

	Package ▼	CVE ▲▼	Severity ▲▼
▶	util-linux 2.29.2-1+deb9u1	CVE-2016-2779	High
▶	tar 1.29b-1.1	CVE-2005-2541	Negligible
▶	systemd 232-25+deb9u4	CVE-2018-6954	High
▶	systemd 232-25+deb9u4	CVE-2018-1049	Medium
▶	systemd 232-25+deb9u4	CVE-2013-4392	Negligible

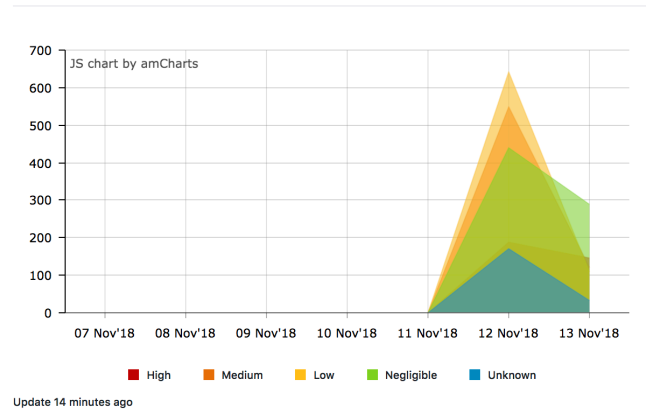


Assessment Metrics

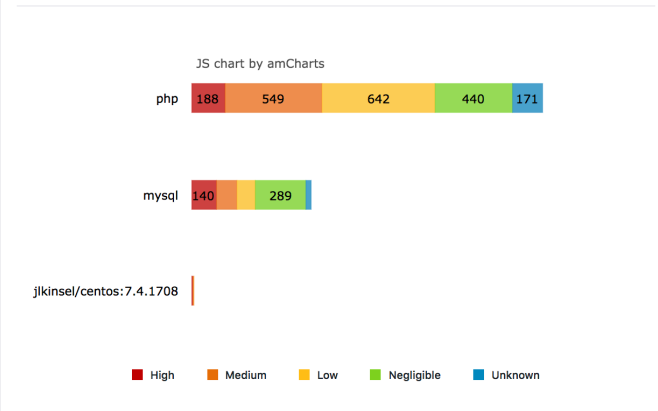
All Vulnerabilities (Last 7 Days)



Vulnerabilities by Severity



Top 5 Most Vulnerable Container Images



All Images (3)

Search



Add Registry

Add Image

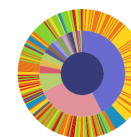
Action ▾

**php**

Scan Status: done

Instrumentation Status: Not Instrumented

Actions ▾

**jlkinsel/centos:7.4.1708**

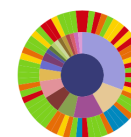
Scan Status: done

Instrumentation Status: Active

Actions ▾

Delete
Instrument

Actions ▾

**mysql**

Scan Status: done

Instrumentation Status: Not Instrumented

Records per page 10 ▾

- [Dashboard](#)
- [Images](#)
- [Vulnerabilities](#)
- [Containers](#)
- [Policies](#)
- [Settings](#)

Metrics **Activity Monitor** Topology

Date Range [Last 7 Days](#)

Top 10 Containers and Images by Activity

Containers Images



Warning 23

High 3

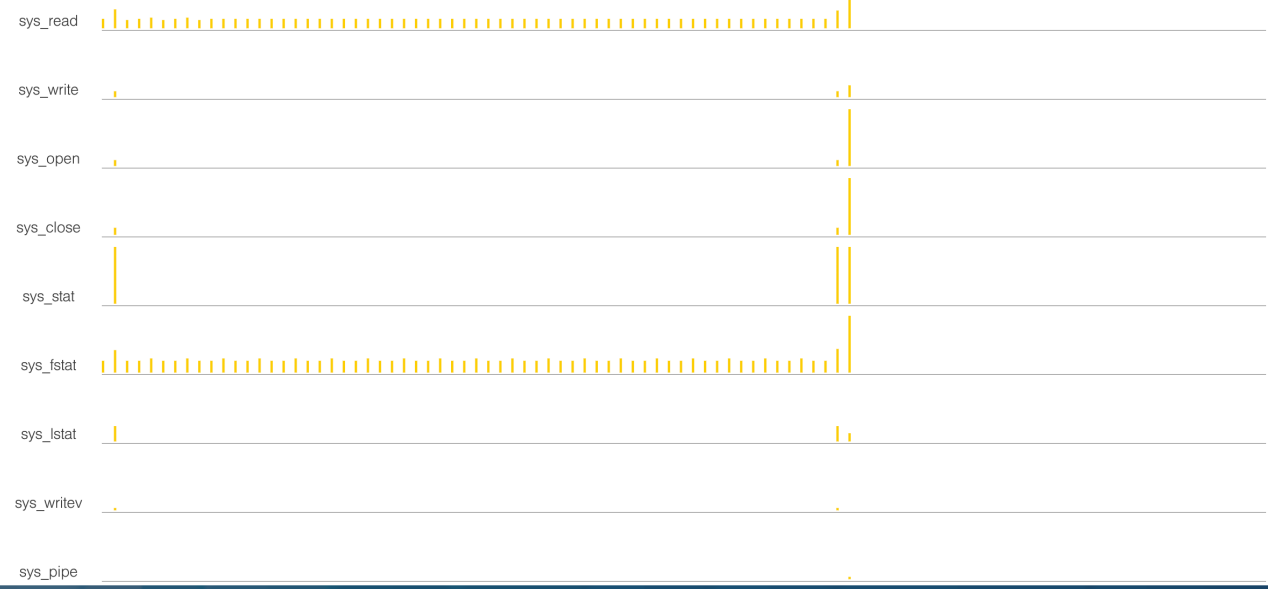
- [Dashboard](#)
- [Images](#)
- [Vulnerabilities](#)
- [Containers](#)
- [Policies](#)
- [Settings](#)

Metrics **Activity Monitor** Topology

Date Range [Last 7 Days](#)

Container Details ?

Just now



Warning 23
High 3

- Dashboard >
- Images >
- Vulnerabilities >
- Containers >
- Policies >
- Settings

Metrics Activity Monitor **Topology**

Date Range 📅 Last 7 Days

Topology Diagram

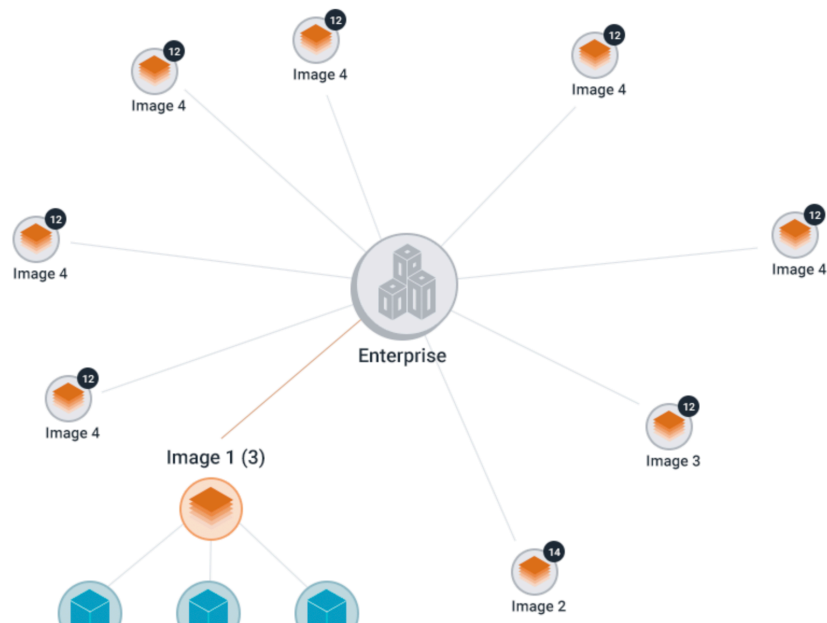
Search



View



Show Geographic Location



Warning 23

High 3

Event Details


Process /usr/sbin/httpd was blocked from executing /bin/sh. Severity: High

Raw log:

Process	Process ID	Call	Arguments	Action	Time
/usr/sbin/httpd	31	sys_execve	/bin/sh	Deny	11/13/2018, 12:48:23AM

Processes executing /usr/sbin/httpd:

- /usr/sbin/httpd

Processes accessing /usr/sbin/httpd:

- /usr/sbin/httpd

Warning 23

High 3



Qualys Container Security (US Only)

By: [Qualys](#)

Latest Version: 1.2.0-196

[Continue to Subscribe](#)[Save to List](#)

Qualys container security provides Inventory, Vulnerability Management, Compliance and Runtime security enabling users to Discover, track and continuously secure containers - from

[Show more](#)

Linux/Unix

★★★★★ (0)

BYOL

[Overview](#)[Pricing](#)[Usage](#)[Support](#)[Reviews](#)

Product Overview

Qualys Container Security (CS), enables customers to build continuous security into their container deployments and DevOps processes at any scale, and integrate the results into one unified view of their global hybrid IT security and compliance posture, breaking down silos and lowering ownership cost. Qualys container security integrates with Jenkins, Bamboo to do Image Vulnerability Analysis. Scan your docker registries like artifactory or ECR either on-demand or with an automated scan of images. Detect potential breaches by scan the running containers and detect drifts from the parent images. Adding Qualys Vulnerability Management and Policy Compliance for the hosts gives you comprehensive coverage of the complete stack. Download the sidecar container sensor image for your specific Qualys platform, follow the instructions and samples templates to deploy across your Build pipeline, EC2, ECS, EKS clusters and get started to gain visibility and security posture of your container environments.

Highlights

- Discover and inventory container assets across your AWS ECS, EKS or custom EC2 container deployments
- Perform container-native vulnerability analysis across Build pipeline like Jenkins, Bamboo, Scan ECR Registry and live container runtimes
- Detect potential breaches in runtimes, where containers are drifting and breaking immutable behavior



QUALYS SECURITY CONFERENCE 2018

Thank You

Hari Srinivasan
hsrinivasan@qualys.com